

EXHIBIT I

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

23 MAG 122

In the Matter of a Warrant for All
Content and Other Information
Associated with Multiple Accounts
Containing Stored Electronic
Communications, USAO Reference
No. 2022R00646

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

BRANDON RACZ, Special Agent, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation for approximately seven years. As an FBI Special Agent, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to an FBI squad in the FBI’s New York Field Office that investigates securities and commodities fraud, along with other white-collar offenses, including market manipulation and insider trading. During my time in the FBI, I have received training about investigating and have participated in investigations financial crimes, including financial crimes related to cryptocurrencies. I have also received training about executing, and have participated in executing, numerous search and seizure warrants involving electronic evidence.

B. The Providers, the Subject Accounts, and the Subject Offenses

2. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 for all content and other information associated with the following accounts and servers (collectively, the “Subject Accounts”):

a. A Twitter account with the username @avi_eisen (“Subject Account-1”) and account ID 2839135427, accessed at the URL https://twitter.com/avi_eisen and maintained and controlled by Twitter (“Provider-1”), headquartered at 1355 Market Street, Suite 900, in San Francisco, California;

b. A Facebook account with the username “Avraham Eisenberg” (“Subject Account-2”), accessed at <https://www.facebook.com/people/Avraham-Eisenberg/100009952574823/> and maintained and controlled by Meta Platforms, Inc. (“Provider-2”), headquartered at 1601 Willow Road, Menlo Park, California 94025; and

c. The following Discord accounts (“Subject Account-3” and “Subject Account-4”) and server (“Subject Server-1”) maintained and controlled by Discord, Inc. (“Provider-3”), headquartered at 444 De Haro Street, Suite 200, San Francisco, CA 94107:

<u>User ID</u>	<u>Username(s)</u>	<u>Referred to Herein As</u>
470697531823620116	AvrahamEisenberg#5451	Subject Account-3
281233046227779585	CrunchWrapSupreme#1469	Subject Account-4

<u>Server ID</u>	<u>Server Link</u>	<u>Referred to Herein As</u>
782504674103656489	discord.gg/9RjPjCdGwK	Subject Server-1

d. The Google accounts associated with the following email addresses, maintained and controlled by Google LLC (“Provider-4”), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA:

- i. bochen.clean@gmail.com (“Subject Account-5”)
- ii. avi@thimessolutions.com (“Subject Account-6”)
- iii. 613ike@gmail.com (“Subject Account-7”)

3. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

4. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1 (commodities fraud); 7 U.S.C. § 13(a)(2) (commodities and swap manipulation); 18 U.S.C. § 371 (conspiracy to commit commodities fraud); 18 U.S.C. §§ 1343 and 1349 (wire fraud, securities fraud, and conspiracy to commit the same); 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957 (concealment money laundering, illegal money transferring, and conspiracy to commit the same), all in connection with a scheme to commit market manipulation on a platform called Mango Markets, then launder the proceeds (the “Subject Offenses”).

5. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of electronic devices and messaging platforms in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Providers

6. I have learned the following about Twitter, which is Provider-1:

a. Twitter offers electronic messaging and online social media services. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to post and read 280-character messages called “tweets,” and to restrict access to their “tweets” to individuals whom they approve. In addition, Twitter's subscribers can send “direct messages,” or “DMs” to other subscribers, which are typically only viewable by the sender and recipient of the direct message. These features are described in more detail below. A subscriber using Twitter's services can access his or her account from any computer or other electronic device connected to the Internet. In addition to content that the user posts, Twitter, like many online social media providers, pulls and stores identifying information when the user is active on the platform, including device identifiers and Internet Protocol (“IP”) addresses of the user’s Internet connection to Twitter.

b. Twitter maintains the following records and information with respect to every subscriber account:

i. *Biographical Information.* Twitter allows its users to create personal profiles pages that are available to the public. These pages may include a short biography, photographs, and location information of the user.

ii. *Subscriber and Billing Information.* Twitter collects and maintains identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Twitter may “verify” some users, displaying a blue checkmark beside the username to affirm to public viewers that the account belongs to the person or entity that claims to operate it. Twitter may request and store verification data on those user accounts it has verified, including copies of government-issued identification documents.

Twitter also maintains records concerning the date the account was created, the IP address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Twitter maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iii. *Tweets.* As discussed above, Twitter's users can use their accounts to post "tweets" of 280 characters or fewer. Each tweet includes a timestamp that displays when the tweet was posted. Twitter's users can also "favorite," "retweet," or reply to tweets of other users, or click a "share" button that allows users to link to the tweet on different outlets, including in private messages. In addition, when a tweet includes a username, often preceded by "@," Twitter designates that tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have favorited or retweeted the user's own tweets, as well as a list of all the tweets that include the user's username (*i.e.*, a list of all mentions and replies for that username). By enabling the "precise location" setting, Twitter's users can also choose to display location data in their tweets.

iv. *Media files.* Twitter users can also include media such as images or videos in their tweets. Each account is provided a user gallery, which stores media files that the user has shared on Twitter's network, including images and videos that were uploaded from another service.

v. *Link Information.* Twitter's users can also include links to a website in their tweets. By using Twitter's linking service, a longer website link can be converted into a shortened link, which allows it to fit into the 280-character limit. The linking service measures how many times a link has been clicked.

vi. *Associated Users.* A user can also “follow” other users, which means that the user subscribes to the other users' tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's “followers” list) and a list of people whom that user follows (i.e., the user's “following” list). Twitter's users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). Limiting account visibility in this way is called “going private.” A user can also group other users into “lists” that display on the right side of the user's home page.

vii. *Direct Messages.* A user can also send direct messages, or DMs, to one of his or her followers, or to other users whose settings accept messages from any Twitter account holder. The user may either click a “share” button on a tweet that generates a direct message to another user that links to that tweet, or the user may start a direct message conversation without linking to a tweet. These messages are visible only to the sender and the recipient. If one party deletes the messages from his or her own account, the message and associated data may still be stored on the other party's account. In addition to retaining content of messages, Twitter retains log data associated with them, analogous to call detail records.

viii. *Search Information.* Twitter has at times included a search function that enables its users to search all public tweets for keywords, usernames, or subject, among other things.

ix. *Third-party Information.* Users can connect their accounts to third-party websites and applications, which may grant these websites and applications access to parts of the users' account data.

x. *Transactional Information.* Twitter also typically retains certain transactional information about the use of each account on its system. This information can include records of logins, such as timestamps of activity, information about the user's device, and IP addresses used to access Twitter. Twitter calls this information "Log Data."

xi. *Customer Correspondence.* Twitter also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account, and including reports and complaints that the subscriber has made to Twitter about other accounts.

xii. *Preserved Records.* Twitter also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

7. I have learned the following about Facebook, which is Provider-2:

a. Meta Platforms, Inc. owns and operates a free-access social networking website called Facebook that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

c. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

d. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or

her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

f. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

g. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

h. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

i. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

j. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

k. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

l. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

m. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

n. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

o. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users

may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

p. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook

“friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

q. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

8. I have learned the following about Discord, which is Provider-3:

a. Discord is a proprietary freeware voice over Internet protocol (VoIP) application for gaming and other online communities. The Discord client was built on the Electron framework using web technologies, which allows it to be multi-platform and run on personal computers and websites. The Discord application has services such as free voice chat servers for users and dedicated server infrastructure, video calling and screen sharing, direct calling, instant messaging, videoconferences, and GameBridge API that allows game developers to support integration with Discord within games. Discord users can create a “server” for free and then invite other users to join the server in order to communicate with another user. A server can be configured as public, meaning anyone can join, or it can be configured to be private. To participate in a private server, a user must be invited by another user who already belongs to that private server. Servers are broken down into subcategories, or “channels,” where users can connect with

each other by chatting or calling. Users can also communicate through direct messages, which are private chats created between 1-10 users.

b. Discord users are able to create and maintain a friends list, participate in multiple servers or communication channels, and set their current status indicator to appear online, away, or invisible to other users. Discord servers can have multiple text-based and voice channels, both public and private. Text messages sent in these channels are persistent, stay visible, and are stored indefinitely. Users are able to communicate in only one channel at a time, but can easily navigate between channels. Discord users are able to direct message or private message to other Discord users. Discord users are able to view what game their Discord friends and other Discord server members are playing.

c. During the registration process for a Discord account, Discord asks subscribers to provide basic client information to include, among other things, a username and email address. Additionally, other online applications like Steam, Facebook, Spotify, and Twitter, can be connected to a user's Discord account. Discord can be used from within a web browser, can be installed on a Windows, Mac, or Linux computer, or can be installed on an Apple iOS or Android mobile device. Discord has an optional paid version called "Discord Nitro" that provides a user with additional features. Therefore, the computers of Discord likely contain information concerning a user's account and their use of Discord services and possibly other connected services, such as account access information, email information, and account application and payment information. Discord also assigns a user identification number to each account. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify and locate the account user(s).

d. Upon creating a Discord account, a Discord user is assigned a unique 18-digit Discord user ID. The Discord user then must create a username (which includes a # and a four-digit number) and an account password. The Discord user may change the username and password without having to open a new Discord account.

e. A subscriber using Discord's services can access his or her account from any computer connected to the Internet or by downloading the desktop or mobile Discord application.

f. In my training and experience, service providers like Discord typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website) and other log files that reflect usage of the account. In addition, service providers often have records of the IP address¹ used to register the account and the IP addresses associated with particular logins to and activity on the account. Because every device that connects to the Internet must use an IP address, IP addresses can help identify which computers or other devices were used to access the account.

¹ An IP address is a unique numeric address used by computers on the Internet. There are two types of IP addresses used on the Internet today. The IPv4 address uses 32 bits and looks like a series of four numbers, each in the range from 0-255, separated by periods - for example 123.4.56.78. Due to the growth of the Internet, the creation of additional IP addresses was needed; therefore, a new version of IP called IPv6, uses 128 bits for IP addresses - for example 2610:0020:6F15:0015:0000:0000:0000:0027, or its abbreviated form of 2610:20:6F15:15::27. Every computer connected to the Internet must be assigned an IP address so that Internet traffic may be directed properly from its source to its destination. Each IP address is uniquely assigned to a single connected device at any single point in time.

g. In some cases, Discord users may communicate directly with Discord about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Discord typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

h. The computers or servers of Discord are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and account activation.

i. Based on the Discord Privacy Policy, last modified February 25, 2022, and available online, I know the following about the collection of preservation of data at Discord:²

i. Discord collects information from users when they voluntarily provide such information, such as when they register for access to the Discord application and related Internet services (the "Services"). Information that Discord collects may include but not be limited to username, email address, and any messages, images, transient VOIP data (to enable communication delivery only) or other content users send via the chat feature.

ii. When users interact with Discord through the Services, Discord receives and stores certain information such as an IP address, device ID, and the user's activities within the Services. Discord may store such information or such information may be included in databases owned and maintained by affiliates, agents or service providers. The Services may use such information and pool it with other information to track, for example, the total number of visitors

² See <https://discordapp.com/privacy> (last accessed March 20, 2022).

to Discord's website, the number of messages users have sent, and the domain names of visitors' Internet service providers.

iii. Discord may conduct research on its customer demographics, interests and behavior based on the information collected. This research may be compiled and analyzed on an aggregate basis, and Discord may share this aggregate data with its affiliates, agents, and business partners. Discord may also disclose aggregated user statistics in order to describe its services to current and prospective business partners, and to other third parties for other lawful purposes.

iv. Users may give Discord permission to collect their information in other services. For example, a user may connect a social networking service ("SNS") such as Facebook or Twitter to their Discord account. When a user does this, it allows Discord to obtain information from those accounts (for example, a user's friends or contacts).

v. Discord employs cookies and similar technologies to keep track of users' local computer's settings such as which account users have logged into and notification settings. Cookies are pieces of data that sites and services can set on a user's browser or device that can be read on future visits. Discord may expand its use of cookies to save additional data as new features are added to the Service. In addition, Discord uses technologies such as web beacons and single-pixel gifs to record log data such as open rates for emails sent by the system.

vi. Discord may use third party web site analytic tools such as Google Analytics on its website that employ cookies to collect certain information concerning use of its Services. However, users can disable cookies by changing their browser settings.

vii. A user may see a Discord Service advertised in other applications or websites. After clicking on one of these advertisements and installing a Discord Service, the user

will become a user of the Service. Advertising platforms, which include Twitter and Facebook (and whose software development kits are integrated within Discord's Service), may collect information for optimizing advertising campaigns outside of the Service.

9. I have learned the following about Google, which is Provider-4:

a. Google offers to the public a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications using a username and password. Once logged into a Google account, a user can connect to Google's full suite of services offered to the general public.

b. In particular, as relevant here, Google offers free, web-based email services to the public. Specifically, Google allows subscribers to maintain email accounts through Gmail under the domain gmail.com and other domain names chosen by the user or an enterprise. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

c. Google maintains the following records and information with respect to every Google account that has email services:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time. Google also allows users to send emails in "confidential" mode, which enables a user to set an expiration date for messages or revoke access at any time,

and recipients of the confidential message will be unable to forward, copy, print, and download the message.

ii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, recovery and alternate email addresses, and sign-in phone numbers. A recovery email address, which can be associated with more than one Gmail account, is used to regain access to an account if a password has been forgotten or a user has been locked out of their account. An alternate email address is a non-Gmail account that a user has provided that can be used to sign into a Gmail account. A sign-in phone number is a phone number that can be used as a primary/additional login identifier to access an account. Google also maintains records concerning the date on which the account was created, the Internet protocol (“IP”)³ address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of Google services utilized by the subscriber. Finally, Google maintains records regarding (1) fetching and forwarding email addresses, which are email accounts from which the primary account receives emails and forwards emails, respectively; (2) email aliases, domain aliases or separate domains associated with the account, which are means by which accounts with other domain names or other email addresses can be associated with a primary Google account; (3) other Google accounts that have access to the primary account, which access can be granted by the user of the primary account; and (4) other email accounts that are associated with the primary Google account.

³ Based on my training and experience, each electronic device connected to the Internet must be assigned an IP address so that communications from or directed to that electronic device are routed properly.

iii. *Device Information.* Google may also collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

iv. *Cookie Data.* Google typically uses features to track the activity of users of its accounts, including whether or not the user of an account accesses other accounts at Google using the same computer or device, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

v. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system, including records of login and logout events relating to Google accounts, including user IP addresses and dates and timestamps.

vi. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

vii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon

receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

j. Google also maintains records with respect to other Google services, which it stores in connection with a Google account and includes the following:

i. *Google Contacts.* Google provides an address book for Google accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Google preserves contacts indefinitely, unless the user deletes them.

ii. *Google Calendar.* Google provides users with the ability to create and maintain online calendars, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars. Google preserves appointments indefinitely, unless the user deletes them.

iii. *Google Messaging Content.* Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user has not disabled that feature or deleted the messages.

iv. *Google Drive content.* Google Drive is a cloud storage service automatically created for each Google account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Google provides users with a certain amount of free storage, currently 15 gigabytes, and users can purchase a storage plan through Google to store additional content. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others and grant those with access the ability to edit or comment. Google maintains a record of who made changes and when to documents edited in Google applications. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and short message service ("SMS") messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive. Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

v. *Google Maps.* Google Maps is service which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. If users log into their Google account while using Google

Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps. Google stores Maps data indefinitely, unless the user deletes it.

vi. *Google Photos*. Google Photos is a cloud-based photo and video storage service through which users can share or receive photos and videos with others. Users have the option to sync their mobile phone or device photos to Google Photos. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google Photos if that data is included by the user as part of the upload. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

vii. *Google Voice*. Google Voice is a service through which a Google account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

viii. *Location History data*. Google collects and retains data about the location at which Google account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. This location data may be associated with the Google account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google account, such as Location History or Web & App Activity tracking. Google

maintains these records indefinitely for accounts created before June 2020, unless the user deletes it. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

ix. *Chrome Browser and “My Activity” Data.* Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user’s browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google account or using the Google Internet search engine available at <http://www.google.com> while logged into their Google account.

k. As explained herein, information stored in connection with a Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Google user’s stored electronic communications, IP logs, and other data retained by Google, can indicate who has used or controlled the Google account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email content, and stored documents and photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Google account at a relevant time. Further, Google account activity can show how and when the account was accessed or used. For example, as described herein, Google logs the IP

addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime(s) under investigation. Such information allows investigators to understand the geographic and chronological context of Google access, use, and events relating to the crime under investigation. Finally, Google account activity may provide relevant insight into the Google account owner's state of mind as it relates to the offense under investigation. For example, information stored in the Google account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting information in an effort to conceal evidence from law enforcement).

D. Jurisdiction and Authority to Issue Warrant

10. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

11. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

12. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as

the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

13. On or about December 13, 2022, the Honorable Gabriel W. Gorenstein authorized a complaint charging AVRAHAM EISENBERG with committing commodities fraud, in violation of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1, and commodities manipulation, in violation of 7 U.S.C. § 13(a)(2), in connection with a scheme to commit market manipulation on a platform called Mango Markets. A copy of the complaint is attached hereto as Exhibit 1 and is incorporated by reference.

14. As explained in the Complaint:

a. Mango Markets is a decentralized cryptocurrency exchange that has its own native crypto token, called MNGO. Investors can buy and sell MNGO and other cryptocurrencies on Mango Markets. Investors on Mango Markets can also buy and sell perpetual futures (“Perpetuals”) based on the relationship between the value of MNGO and the value of a crypto stablecoin called USD Coin (“USDC”), which is designed to be pegged to the dollar. Perpetuals are “swaps” under the Commodity Exchange Act. An investor who buys a Perpetual for MNGO stands to profit if the value of MNGO rises relative to the value of USDC, and an investor who sells a Perpetual for MNGO stands to profit if the value of MNGO falls relative to the value of USDC. Finally, Mango Markets allows investors to borrow cryptocurrency from the exchange, in amounts based on the value of the borrower’s portfolio, and to withdraw that borrowed cryptocurrency. Compl. ¶¶ 4, 7-8.

b. In or about October 2022, AVRAHAM EISENBERG participated in a scheme to steal approximately \$110 million by artificially manipulating the price of MNGO Perpetuals on

Mango Markets (the “Market Manipulation Scheme”). The scheme worked as follows: EISENBERG used an account that he controlled on Mango Markets to sell a large amount of Perpetuals for MNGO and used a separate account on Mango Markets to purchase those same Perpetuals. In other words, EISENBERG sold himself MNGO Perpetuals. EISENBERG then engaged in a series of large purchases of MNGO, with the objective of artificially increasing the price of MNGO relative to USDC, which had the effect of increasing the price of MNGO Perpetuals on Mango Markets. That purchasing achieved the desired effect, causing the price of MNGO Perpetuals on Mango Markets to increase precipitously over the course of approximately 20 minutes. Over that time span of approximately 20 minutes, the price of MNGO Perpetuals rose from approximately 0.0382 USDC/MNGO to approximately 0.54 USDC/MANGO, an increase of approximately 1300 percent. Compl. ¶¶ 5, 9-17.

c. As the price of MNGO Perpetuals on Mango Markets rose as a result of the Market Manipulation Scheme perpetrated by AVRAHAM EISENBERG the value of the MNGO Perpetuals that EISENBERG had purchased also rose. Because Mango Markets allows investors to borrow and withdraw cryptocurrency based on the value of their assets on the platform, the increase in the value of the MNGO Perpetuals EISENBERG had purchased allowed EISENBERG to borrow, then withdraw, approximately \$110 million worth of various cryptocurrencies from Mango Markets, which came from deposits of other investors in the Mango Markets exchange. When EISENBERG borrowed and withdrew that cryptocurrency, he had no intention to repay the borrowed funds. Accordingly, after EISENBERG borrowed and withdrew essentially all of the cryptocurrency deposits on the Mango Markets platform, EISENBERG ceased manipulating the price of MNGO Perpetuals, causing the price of MNGO Perpetuals to fall significantly. Due to

EISENBERG's withdrawals, other investors with deposits on Mango Markets lost much, or all, of those deposits. Compl. ¶¶ 5, 9-17.

15. As explained in the Complaint, virtual currencies, such as USDC, are “commodities” under the Commodity Exchange Act (“CEA”). See, e.g., *C.F.T.C. v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018) (“A ‘commodity’ encompasses virtual currency both in economic function and in the language of the statute.”); *United States v. Reed*, No. 20 Cr. 500 (JGK), 2022 WL 597180, at *3 (S.D.N.Y. Feb. 28, 2022) (finding “defendant had ample notice from the broad definition of commodities under the CEA that cryptocurrencies were within the definition of commodities”). Accordingly, Perpetuals based on the relative value of MNGO and USDC are “swaps” under the CEA. See 7 U.S.C. § 1(47)(A).

16. Based on the foregoing, and the information in the Complaint, I respectfully submit there is probable cause to believe that AVRAHAM EISENBERG engaged in the Subject Offenses.⁴

B. Probable Cause Regarding the Subject Accounts and the Subject Servers

17. As explained below, there is probable cause to believe that the Subject Accounts and the Subject Servers will contain evidence of the Subject Offenses.

Subject Account-1 – Twitter Account

18. As explained above, **Subject Account-1** is a Twitter account with the username @avi_eisen (“Subject Account-2”), accessed at the URL https://twitter.com/avi_eisen.

19. There is probable cause to believe AVRAHAM EISENBERG uses **Subject Account-**

⁴ Although the Complaint only charges commodities fraud and commodities manipulation, I respectfully submit that there is probable cause to believe that the conduct described in the Complaint and in this Affidavit also constitutes wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349, money laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957, and conspiring to commit those offenses.

1 because it has his name in the username and has, in the past, displayed a user photograph that I know was an image of EISENBERG based on my review of his passport photograph and other images of him.

20. Based on my review of publicly available posts on Twitter, there is probable cause to believe that **Subject Account-1** contains evidence of EISENBERG's involvement in the Market Manipulation Scheme. Specifically:

a. As explained above, on or about October 15, 2022, **Subject Account-1** displayed a post in which EISENBERG stated, in substance and in part, that he and others "operated a highly profitable trading strategy last week" that "took place on[] Mango Markets" and resulted in Mango Markets becoming "insolvent."

b. On or about October 20, 2022, **Subject Account-1** also displayed a post stated, in part, that "Mango used switchboard, not Pyth." Based on my review of publicly available records about Mango Markets, I understand that this is a reference to the type of "oracle" used by Mango Markets for setting the price of Perpetuals.

21. Moreover, based on my review of publicly available posts on Twitter, I have learned, in substance and in part, that **Subject Account-1** displays multiple posts of Department of Justice announcements related to financial fraud, including market manipulation, which is evidence that EISENBERG knew he was breaking the law when he committed the Market Manipulation Scheme.

22. Finally, based on my training and experience, and as explained above, I know that in addition to making public posts, Twitter users can also exchange "direct messages" with one another that are not publicly available. There is probable cause to believe that EISENBERG uses the direct messaging function because, based on my review of publicly available Twitter posts, I

know that **Subject Account-1** has posted tweets that contain numerous references to EISENBERG communicating through “DM,” which is a commonly used abbreviation for direct messaging.

Subject Account-2 – Facebook Account

23. As explained above, **Subject Account-2** is a Facebook account with the username “Avraham Eisenberg”, accessed at <https://www.facebook.com/people/Avraham-Eisenberg/100009952574823/>.

24. There is probable cause to believe that AVRAHAM EISENBERG uses **Subject Account-2** because the username is his name and publicly available photographs show EISENBERG, whom I recognize from reviewing EISENBERG’s passport photograph and other images and videos of him.

25. There is probable cause to believe **Subject Account-2** will contain evidence of the Subject Offenses. Based on my participation in an interview of an individual (“Individual-1”) who contacted law enforcement following the Market Manipulation Scheme,⁵ I have learned, in substance and in part, the following:

a. Individual-1 met EISENBERG online approximately two years ago through Facebook. Individual-1 identified **Subject Account-2** as EISENBERG’s Facebook account. Individual-1 and EISENBERG had shared mutual interests, so they communicated with one another over, among other things, Facebook Messenger (which is Facebook’s messaging tool), Discord, and an encrypted messaging application called Signal.

b. EISENBERG communicated about the Market Manipulation Scheme before and after carrying it out on a Discord server called “CSP Trading,” which is **Subject Server-1** and

⁵ Individual-1 stated, in substance and in part, that Individual-1 was involved in cryptocurrency trading and was interested in potentially receiving compensation for providing information to law enforcement.

is discussed in greater detail below. EISENBERG deleted some of his messages from **Subject Server-1** after carrying out the Market Manipulation Scheme. Individual-1 described to me **Subject Server-1** and identified some of the places where EISENBERG had deleted messages.

c. EISENBERG typically communicated with Individual-1 over Facebook and an encrypted messaging application called Signal. Individual-1's communications with EISENBERG included communications about Mango Markets and EISENBERG leaving the country to Israel after committing the Market Manipulation Scheme because he was afraid of prosecution. Individual-1 believed that these communications may have occurred on Signal, but was unsure.⁶

d. Individual-1 also stated that EISENBERG communicated with Individual-1 and others over Facebook about cryptocurrency trading, including trading for which, I know based on publicly available records from Twitter and Discord, EISENBERG had been accused of fraud and market manipulation.

26. Based on my communications with other law enforcement officers and my review of travel records, I have corroborated that, on or about October 12, 2022—right after the Mango Market manipulation scheme—EISENBERG traveled from the United States to Israel, then returned to the United States on or about December 26, 2022.

Subject Accounts-3 to -4 and Subject Server-1– Discord Accounts and Server

27. Based on my training and experience, and as explained above, Discord is an online

⁶ Individual-1 stated, in substance and in part, that Individual-1 had taken screenshots and screen recordings of his communications with EISENBERG about the Mango Market manipulation scheme. Individual-1 stated that Individual-1 would send me those screenshots and recordings, but has not done so. Individual-1 also stated, in substance and in part, that he did not know whether EISENBERG worked with others in committing the Subject Offenses, but believed EISENBERG worked alone.

service that is, among other things, a messaging platform where users can exchange text or voice messages. Discord users can create a “server” for free and then invite other users to join the server in order to communicate with another user. A server can be configured as public, meaning anyone can join, or it can be configured to be private. To participate in a private server, a user must be invited by another user who already belongs to that private server. Servers are broken down into subcategories, or “channels,” where users can connect with each other by chatting or calling.

28. As explained above, **Subject Server-1** is a Discord server available at discord.gg/9RjPjCdGwK and with Server ID 782504674103656489.

29. Based on my review of messages from **Subject Server-1** and data from Discord, I have learned, in substance and in part, the following:

a. **Subject Server-1** is named “CSP Trading,” and that it contains multiple channels where users post messages.

b. Numerous users post messages on **Subject Server-1**’s channels, including:

- (i) the user of **Subject Account-3**, which has the username AvrahamEisenberg#5451, the user ID 470697531823620116, and also uses the vanity name “Vires Creditor and Honest Person”; and
- (ii) the user of **Subject Account-4**, which has the username CrunchWrapSupreme#1469 and the user ID 281233046227779585 and also uses the vanity name “CSP Trading.”

c. There is probable cause to believe that EISENBERG uses **Subject Account-3** because, among other things, the username contains his name and the account lists the same address listed on a cryptocurrency account at Circle (identified in the Complaint as “Circle Account-1”) that, as explained in the Complaint, I know EISENBERG uses because he provided his passport to open the account.

30. Based on my review of messages from **Subject Server-1**, there is probable cause to

believe that **Subject Server-1** will contain evidence of the Subject Offenses for, among other things, the following reasons:

a. On or about October 11 and October 12, 2022, multiple users on **Subject Server-1** wrote posts accusing EISENBERG, who was a regular poster on **Subject Server-1**, of being responsible for the Mango Market manipulation scheme.

b. On or about October 12, 2022, **Subject Account-3** made multiple posts on **Subject Server-1** making fun of Mango Markets. For example, at approximately 4:36 a.m., **Subject Account-3** posted a screenshot of a tweet from another user stating “Apple made \$94 billion last year[,] Mangos lost \$115 million today[,] Investing in fruit is unpredictable.” Similarly, at approximately 4:43 a.m., **Subject Account-3** posted a link to a reddit page about the Mango Markets manipulation scheme and wrote, in part, “Comments here pretty positive . . . the mango discord suffers from selection bias.”

c. **Subject Account-3** continued to post regularly on **Subject Server-1** through the rest of October, including about the Mango Markets manipulation scheme. For example:

i. On or about October 16, 2022, at approximately 10:25 p.m., **Subject Account-3** posted: “Protip: always make sure your odds of being a billionaire is greater than odds of being in jail[.] And you’ll do fine.”

ii. On or about October 17, 2022, at approximately 10:59 p.m., **Subject Account-3** posted a series of messages about having more Twitter followers than a leader of Mango Labs, which built Mango Markets.

iii. On or about October 19, 2022, at approximately 10:19 p.m., **Subject Account-3** posted a screenshot of odds about EISENBERG’s future, including, among others, “[w]hich protocol will Avraham Eisenberg plunder next” and “[w]ill Avraham Eisenberg spend at

least 6 months in jail before the end of 2030.”

iv. On or about October 20, 2022, at approximately 12:25 a.m., **Subject Account-3** posted a link to a Tweet about the Mango Market manipulation scheme being entertaining, followed by the text: “It’s amazing how much funnier you get after you have 47 million dollars.”

v. On or about October 22, 2022, at approximately 6:50 p.m., **Subject Account-3** posted a link to a Tweet about an individual (“Individual-2”) calling the Mango Markets manipulation scheme “market manipulation,” followed by the text: “Big talk from market manipulator [Individual-2]” and asking for a link to information about Individual-2’s market manipulation scheme.

vi. On or about October 25, 2022, at approximately 8:09 a.m., **Subject Account-3** tweeted a link to a podcast in which EISENBERG was interviewed about the Mango Market manipulation scheme.

31. There is also probable cause to believe that **Subject Accounts-3 and -4** contain evidence of the Subject Offenses, including in posts on servers other than **Subject Server-1**. Specifically, based on my review of messages on **Subject Server-1** and on a public article about the Mango Market manipulation scheme, I have learned, in substance and in part, the following:

a. As explained above, EISENBERG used **Subject Account-3** and used that account to post frequently about the Mango Market manipulation scheme on **Subject Server-1**. Based on my training and experience, I know that individuals who use Discord often post on multiple servers, including private servers, because it allows them to talk with different groups of people or with specific individuals. Accordingly, there is probable cause to believe that **Subject Account-3** contains communications about the Subject Offenses beyond what is available on

Subject Server-1.

b. Consistent with my training and experience, there is probable cause to believe **Subject Account-3** communicated separately with **Subject Account-4** about efforts to cover up EISENBERG's planning for the Mango Market manipulation scheme. Specifically:

i. On or about October 12, 2022—which is after the Mango Market manipulation scheme but before EISENBERG admitted his involvement in that scheme—a publicly available post on Substack, which is a blogging platform, accused EISENBERG of committing the exploit and posted what appear to be messages from Discord, in which **Subject Account-3** posted about some of the steps that EISENBERG later took in carrying out the Mango Market manipulation scheme.

ii. **Subject Server-1** contains portions of the messages in the screen shots described above, but not all of them, and has notations that certain messages have been deleted. Based on my training and experience and my review of Discord servers, I understand this means that some of the messages that appeared on screenshots in the blog post described above were likely deleted.

c. Consistent with my training and experience, multiple users on **Subject Server-1** posted about incriminating messages from **Subject Account-3** being deleted from **Subject Server-1**. Those users accused the user of **Subject Account-4**, who was a moderator of **Subject Server-1**, of deleting messages at EISENBERG's request.

d. When confronted with these accusations, the user of **Subject Account-4** did not deny them and, at times, defended EISENBERG. For example:

i. On or about October 12, 2022, at approximately 12:20 a.m., a user who had posted screenshots of **Subject Account-3**'s posts that appeared on the blog post described above

wrote a post directed at **Subject Account-4** asking, in substance and in part, whether **Subject Account-4** had deleted the screenshots. **Subject Account-4** cryptically responded, “go padres,” then wrote “I hear hes already fled the usa.”

ii. On or about October 12, 2022, at approximately 12:26 a.m., a different user asked, in substance and in part, why **Subject Account-4** would be deleting messages for EISENBERG. Approximately one minute later, **Subject Account-4** wrote: “avi did nothing wrong,” using a shorthand for EISENBERG’s first name.

iii. On or about October 12, 2022, at approximately 1:42 a.m., after additional attempts by other users to re-post **Subject Account-3**’s incriminating messages, **Subject Account-4** posted: “[T]his should be a safe collaborative space to say what ur working on [without] worrying about people taking screenshots and posting them elsewhere,” in an apparent reference to the blog post described above.

e. Based on my training and experience, the fact that the user of **Subject Account-4** appears to have been deleting messages from **Subject Server-1** for EISENBERG and appears to have known that EISENBERG left the United States shortly after the Mango Market manipulation scheme suggests that the users of **Subject Account-4** was communicating separately with EISENBERG about the aftermath of the Mango Market manipulation scheme.

Subject Accounts-5 to -7 – Google Accounts

32. As explained above, **Subject Account-5** is a Google account associated with the email address bochen.clean@gmail.com, **Subject Account-6** is a Google account associated with the email address avi@thimesolutions.com, and **Subject Account-7** is a Google account associated with the email address 613ike@gmail.com.

33. I have learned that **Subject Account-5** was used to perpetrate the Market Manipulation

Scheme. Specifically, based on my review of records from a cryptocurrency exchange (identified in the Complaint and herein as “Exchange-1”), as well as my review of records from Google, I have learned, in substance and in part, the following:

a. As explained in the Complaint, on or about September 19, 2022, an account (identified in the Complaint and herein as the “Exchange-1 Account”) was opened at Exchange-1, using a passport and personal identifying information that appears to belong to a Ukrainian woman, along with the email address for **Subject Account-5**. *See* Comp. ¶ 14.

b. As explained in the Complaint, the Exchange-1 Account received over 12 million USDC from Circle Account-1, which is EISENBERG’s account at Circle, then sent a large portion of those funds to other cryptocurrency wallets that EISENBERG used to carry out the Market Manipulation Scheme. *See* Compl. ¶ 10.

c. Moreover, as explained in the Complaint, the Exchange-1 Account purchased a large quantity of MNGO using USDC, as part of EISENBERG’s effort to manipulate the price of MNGO Perpetuals in the Market Manipulation Scheme. *See* Compl. ¶ 14.

34. I have also learned that EISENBERG appears to control the Exchange-1 Account and **Subject Account-5**, as well as **Subject Accounts-6 and -7**. Specifically, based on my review of records from Google, I have learned, in substance and in part, the following:

a. As explained above, Circle Account-1, which is EISENBERG’s account, sent over 12 million USDC to the Exchange-1 Account. Based on my training and experience, I know that one account sending such a large amount of cryptocurrency to another account, without appearing to receive any cryptocurrency in return, is often strong evidence that the same individual owns both cryptocurrency accounts.

b. As explained above, the Exchange-1 Account was created on or about

September 19, 2022, using the email address for **Subject Account-5** as the email address for the account. Based on my review of records from Google, I have learned that **Subject Account-5** was created on or about September 1, 2022 – just a few weeks before the Exchange-1 Account was opened. Based on my training and experience, I know that individuals who commit financial fraud online often create new email accounts specifically for the criminal scheme, and the short period of time between **Subject Account-5** opening and the Market Manipulation Scheme is strong evidence that **Subject Account-5** was created specifically for the crime.

c. Google records show that the recovery email address for **Subject Account-5** is the email address for **Subject Account-6**, which is registered to “Avi Eisenberg.” Based on my participation in this investigation, I know that “Avi” is one of EISENBERG’s nicknames. Moreover, **Subject Account-6** has, as a recovery email address, **Subject Account-7**, which is also registered to “Avraham Eisenberg.” Finally, **Subject Account-5**, **Subject Account-6**, and **Subject Account-7** all have the same phone number (“Phone Number-1”) listed as the recovery phone number.

d. Phone Number-1 is also listed as the contact phone number for Circle Account-1, which I know is EISENBERG’s account for the reasons given in the Complaint.

e. Accordingly, there is probable cause to believe that EISENBERG controls **Subject Accounts-5** through **-7**.

35. There is probable cause to believe **Subject Accounts-5** through **-7** will contain evidence of, and are instrumentalities of, the Subject Offenses, for the following reasons:

a. As explained above, **Subject Account-5** is the email address listed for the Exchange-1 Account, which was used to perpetrate the Market Manipulation Scheme. Data from **Subject Account-5** – including emails, payment information, chat records, location data, IP data,

and any saved documents or photographs – will provide information about the identity of the individual or individuals who created and used **Subject Account-5**, including to set up and access the Exchange-1 Account.

b. Similarly, as explained above, **Subject Account-6** is listed as the recovery email address for **Subject Account-5**. Data from **Subject Account-6** – including emails, payment information, chat records, location data, IP data, and any saved documents or photographs – will provide information about the identity of the individual or individuals who created and used **Subject Account-5**, including to set up and access the Exchange-1 Account. Moreover, because **Subject Account-6** preceded **Subject Account-5** and, as explained above, it appears that EISENBERG created **Subject Account-5** to commit the Market Manipulation Scheme using someone else’s identity, there is probable cause to believe **Subject Account-6** will contain communications, documents, chats, and other records about the Market Manipulation Scheme, decision to use **Subject Account-5** rather than **Subject Account-6**, and efforts to obtain the personal identifying information used to create **Subject Account-5** and the Exchange-1 Account.

c. Additionally, as explained above, EISENBERG controls **Subject Account-7** and listed that account as the recovery email address for **Subject Account-6**. Google records show that **Subject Account-7** includes a “Google Voice” account for Phone Number-1. As explained above, Phone Number-1 is listed as the contact phone number for **Subject Account-6**, **Subject Account-5**, and Circle Account-1. Accordingly, data from **Subject Account-7** – including emails, payment information, chat records, location data, IP data, and any saved documents or photographs – will provide information about the identity of the user of Phone Number-1 and, therefore, the users of **Subject Account-6**, **Subject Account-5**, and Circle Account-1.

d. Google records show that the user of **Subject Account-7** (who, as explained

above, is believed to be EISENBERG) accessed **Subject Account-7** in the days leading up to the Market Manipulation Scheme, the day of the Market Manipulation Scheme, and the days after the Market Manipulation Scheme. That access included using Phone Number-1 to send and receive phone calls, receive voice messages, and send and receive text messages. As explained above and in the Complaint, I know that EISENBERG communicated with others about the Market Manipulation Scheme both before and after the crime, and that he publicly referred to committing the Market Manipulation Scheme with a team. Accordingly, there is probable cause to believe that **Subject Account-7** will contain communications about the Subject Offenses, as well as information that will help identify any co-conspirators in the Subject Offenses.

36. Finally, based on my training and experience, I know that individuals involved in financial crimes often use Google accounts, such as **Subject Accounts-5** through **-7**, to receive, send, and store financial information, including information about bank accounts and cryptocurrency accounts. Individuals also often use Google accounts to receive, send, store, and maintain ledgers and documents, including ledgers containing information about the location of assets and documents reflecting research about cryptocurrency platforms and potential fraud schemes.

37. For the foregoing reasons, there is probable cause to believe that **Subject Accounts-5** through **-7** will contain evidence of, and are instrumentalities of, the Subject Offenses.

38. **Time Limitation.** As described above, the Market Manipulation Scheme took place principally on or about October 11, 2022, when the trades and movements of cryptocurrency discussed above were executed. Based on my training and experience and my participation in this investigation, I know that the Market Manipulation Scheme likely took months to plan because it required millions of dollars' worth of cryptocurrency and a detailed understanding of complicated

facts about Mango Markets, such as the prices used by the Mango Markets “oracle” and the amount of MNGO purchasing needed to significantly increase the price of MNGO Perpetuals. Moreover, based on my training and experience and my participation in this investigation, I know that EISENBERG likely continued to create evidence of the Market Manipulation Scheme for months after October, both through moving the proceeds of that offense and discussing it with others, including in the podcasts described above. Accordingly, I respectfully request that the warrants authorize the collection of data from July 1, 2022 to the present.

C. Evidence, Fruits and Instrumentalities

39. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers’ servers associated with the Subject Accounts and the Subject Server will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant, which is incorporated by reference herein.

40. In particular, I believe the Subject Accounts and the Subject Server are likely to contain the following information:

- a. Records relating to the creation and users of the Subject Accounts and the Subject Servers;
- b. Evidence of the creation and use of cryptocurrency wallets and accounts on cryptocurrency exchanges used in preparing for, perpetrating, or receiving funds from the Subject Offenses;
- c. Evidence, including documents, images, and communications, reflecting any preparation for the Subject Offenses, including but not limited evidence reflecting research about manipulating cryptocurrency prices; research about potential targets for market manipulation; tests of purchasing and selling MNGO or MNGP Perpetuals; tests of transferring cryptocurrency to and

from Mango Markets and other cryptocurrency exchanges used in the Subject Offenses; the planned steps in the Subject Offenses; the anticipated timing of the Subject Offenses; and planning for laundering funds from the Subject Offenses;

d. Evidence, including documents, images, and communications, reflecting acts in furtherance of the Subject Offenses and the transfer of funds obtained from the Subject Offenses;

e. Evidence, including documents, images, and communications, reflecting efforts to avoid to destroy or conceal information about the Subject Offenses, including but not limited to efforts to delete messages about the Subject Offenses and to prevent victims of the Subject Offenses from reporting information about the scheme to law enforcement;

f. Evidence, including documents, images, and communications, relating to AVRAHAM EISENBERG's relocation from the United States to Israel shortly after committing the Subject Offenses;

g. Evidence, including documents, images, and communications, reflecting AVRAHAM EISENBERG's knowledge of the laws prohibiting wire fraud, securities fraud, commodities fraud, and market manipulations, including but not limited to evidence of EISENBERG's participation in lawsuits involving laws related to those subjects and EISENBERG's research or communication about lawsuits and criminal cases related to those subjects;

h. Evidence reflecting the identities of, and communications among, any co-conspirators in the Subject Offenses;

i. Evidence, including documents and communications, reflecting the state of mind of AVRAHAM EISENBERG and other participants in the Subject Offenses, including

communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses;

j. Information that would assist in identifying and locating victims or witnesses;

k. Documents, spreadsheets, communications, and ledgers tracking cryptocurrency transfers and/or cryptocurrency payments;

l. Passwords or other information needed to access or identify computer or other online accounts, storage media, or other places where additional evidence, fruits, or instrumentalities of the Subject Offenses may be located;

m. Information pertaining to cryptocurrency digital wallets that may contain proceeds of the Subject Offenses;

n. Information relating to the ownership and disposition of criminal proceeds, including bank accounts, cryptocurrency wallets, accounts with centralized cryptocurrency exchanges, and other financial accounts;

o. Evidence relating to the use of financial accounts and transactions in furtherance of the Subject Offenses (including the means and methods used to obtain the accounts and funds therein, and how the transactions were undertaken);

p. Evidence concerning the technical expertise of AVRAHAM EISENBERG and any other participants in the Subject Offenses;

q. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place AVRAHAM EISENBERG and any co-conspirators and aiders and abettors in the Subject Offenses, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

r. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, payment for such online facilities or services, transfers of funds in furtherance of the Subject Offenses, and proceeds of the Subject Offenses; and

s. Evidence concerning any other online accounts, any computer devices or servers, or any other location where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

2. In addition to there being probable cause that the Subject Accounts and Subject Server contain evidence of the Subject Offenses, there is also probable cause to believe that they are instrumentalities of the Subject Offenses. Based on my training and experience, my conversations with other law enforcement officers, and my participation in this investigation, I know that when an individual uses electronic accounts to engage in financial crimes, including market manipulation, those accounts will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime. The accounts are instrumentalities of the crime because they were a means of committing the criminal offense.

III. Review of the Information Obtained Pursuant to the Warrant

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and

instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

42. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

43. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. The targets of this investigation include sophisticated computer users who known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's

investigation. *See* 18 U.S.C. § 2705(b)(3). In light of my background and experience, I know that in many cyber investigations, targets have destroyed internet infrastructure and deleted accounts and servers upon learning that the infrastructure may have been identified as being part of the criminal scheme. *See* 18 U.S.C. § 2705(b)(3).

44. Accordingly, there is reason to believe that, were the Providers to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Providers not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

45. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

V. Conclusion

46. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C.

§ 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

/s authorized electronic signature

BRANDON RACZ
Special Agent, FBI

Sworn to me through the transmission of this
Affidavit through reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1,
this 6t day of January, 2023

A handwritten signature in black ink, appearing to read 'S. Netburn', written over a horizontal line.

HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

23 MAG 122

In the Matter of a Warrant for All
Content and Other Information
Associated with a Twitter Account
with Username @avi_eisen,
Maintained at Premises Controlled by
Twitter, Inc., USAO Reference No.
2022R00646

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Twitter Inc. (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent Brandon Racz of the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that a Twitter account with the username @avi_eisen (the “Subject Account”) and account ID 2839135427, accessed at the URL https://twitter.com/avi_eisen and maintained and controlled by Twitter Inc., headquartered at 1355 Market Street, Suite 900, in San Francisco, California, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

01/06/2023

Date Issued

5:08 p.m.

Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Twitter Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Twitter, Inc. (the “Provider”), headquartered at headquartered at 1355 Market Street, Suite 900, in San Francisco, California, and applies to all content and other information within the Provider’s possession, custody, or control associated with a Twitter account with the username @avi_eisen and account ID 2839135427, accessed at the URL https://twitter.com/avi_eisen (the “Subject Account”). A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A, for the period from **July 1, 2022 to the present**:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;

- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- f. All “Tweets” and Direct Messages sent, received, “favorited,” or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;
- g. All photographs and images in the user gallery for the account;
- h. All location data associated with the account, including all information collected by the “Tweet With Location” service;
- i. All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- j. All data and information that has been deleted by the user;
- k. A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list);
- l. A list of all users that the account has “unfollowed” or blocked;
- m. All “lists” created by the account;
- n. All information on the “Who to Follow” list for the account;
- o. All privacy and account settings;
- p. All records of Twitter searches performed by the account, including all past searches saved by the account;

q. All information about connections between the account and third-party websites and applications;

r. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under Government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1 (commodities fraud); 7 U.S.C. § 13(a)(2) (commodities and swap manipulation); 18 U.S.C. § 371 (conspiracy to commit commodities fraud); 18 U.S.C. §§ 1343 and 1349 (wire fraud, securities fraud, and conspiracy to commit the same); 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957 (concealment money laundering, illegal money transferring, and conspiracy to commit the same), all in connection with a scheme to commit market manipulation on a platform called Mango Markets, then launder the proceeds (the "Subject Offenses"), including the following:

a. Records relating to the creation and users of the Subject Accounts and the Subject Servers;

b. Evidence of the creation and use of cryptocurrency wallets and accounts on cryptocurrency exchanges used in preparing for, perpetrating, or receiving funds from the Subject Offenses;

c. Evidence, including documents, images, and communications, reflecting any preparation for the Subject Offenses, including but not limited evidence reflecting research about

manipulating cryptocurrency prices; research about potential targets for market manipulation; tests of purchasing and selling MNGO or MNGP Perpetuals; tests of transferring cryptocurrency to and from Mango Markets and other cryptocurrency exchanges used in the Subject Offenses; the planned steps in the Subject Offenses; the anticipated timing of the Subject Offenses; and planning for laundering funds from the Subject Offenses;

d. Evidence, including documents, images, and communications, reflecting acts in furtherance of the Subject Offenses and the transfer of funds obtained from the Subject Offenses;

e. Evidence, including documents, images, and communications, reflecting efforts to avoid to destroy or conceal information about the Subject Offenses, including but not limited to efforts to delete messages about the Subject Offenses and to prevent victims of the Subject Offenses from reporting information about the scheme to law enforcement;

f. Evidence, including documents, images, and communications, relating to AVRAHAM EISENBERG's relocation from the United States to Israel shortly after committing the Subject Offenses;

g. Evidence, including documents, images, and communications, reflecting AVRAHAM EISENBERG's knowledge of the laws prohibiting wire fraud, securities fraud, commodities fraud, and market manipulations, including but not limited to evidence of EISENBERG's participation in lawsuits involving laws related to those subjects and EISENBERG's research or communication about lawsuits and criminal cases related to those subjects;

h. Evidence reflecting the identities of, and communications among, any co-conspirators in the Subject Offenses;

- i. Evidence, including documents and communications, reflecting the state of mind of AVRAHAM EISENBERG and other participants in the Subject Offenses, including communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses;
- j. Information that would assist in identifying and locating victims or witnesses;
- k. Documents, spreadsheets, communications, and ledgers tracking cryptocurrency transfers and/or cryptocurrency payments;
- l. Passwords or other information needed to access or identify computer or other online accounts, storage media, or other places where additional evidence, fruits, or instrumentalities of the Subject Offenses may be located;
- m. Information pertaining to cryptocurrency digital wallets that may contain proceeds of the Subject Offenses;
- n. Information relating to the ownership and disposition of criminal proceeds, including bank accounts, cryptocurrency wallets, accounts with centralized cryptocurrency exchanges, and other financial accounts;
- o. Evidence relating to the use of financial accounts and transactions in furtherance of the Subject Offenses (including the means and methods used to obtain the accounts and funds therein, and how the transactions were undertaken);
- p. Evidence concerning the technical expertise of AVRAHAM EISENBERG and any other participants in the Subject Offenses;
- q. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place AVRAHAM EISENBERG and any co-conspirators and aiders and abettors in the Subject Offenses, as well as the devices they

used, in specific places at specific times, and would indicate the use of their devices during those times;

r. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, payment for such online facilities or services, transfers of funds in furtherance of the Subject Offenses, and proceeds of the Subject Offenses; and

s. Evidence concerning any other online accounts, any computer devices or servers, or any other location where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with a Facebook Account
with Username “Avraham Eisenberg,”
Maintained at Premises Controlled by
Meta Platforms, Inc., USAO Reference
No. 2022R00646

23 MAG 122

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Meta Platforms, Inc. (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent Brandon Racz of the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that a Facebook account associated with the username “Avraham Eisenberg” (the “Subject Account”), accessed at <https://www.facebook.com/people/Avraham-Eisenberg/100009952574823/> and maintained and controlled by Meta Platforms, Inc. (the “Provider”), headquartered at 1601 Willow Road, Menlo Park, California 94025, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order

may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

01/06/2023

5:09 p.m.

Date Issued

Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Facebook Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Meta Platforms, Inc. (the “Provider”), headquartered at 1601 Willow Road, Menlo Park, California 94025, and applies to all content and other information within the Provider’s possession, custody, or control associated with a Facebook account associated with the username “Avraham Eisenberg”, accessed at <https://www.facebook.com/people/Avraham-Eisenberg/100009952574823/> (the “Subject Account”). A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account listed in Attachment A, for the period from **July 1, 2022 to the present**:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

d. All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

f. All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

g. All "check ins" and other location information;

h. All IP logs, including all records of the IP addresses that logged into the account;

i. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

j. All information about the Facebook pages that the account is or was a "fan" of;

k. All past and present lists of friends created by the account;

- l. All records of Facebook searches performed by the account;
- m. All information about the user's access and use of Facebook Marketplace;
- n. The types of service utilized by the user;
- o. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- p. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- q. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under Government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1 (commodities fraud); 7 U.S.C. § 13(a)(2) (commodities and swap manipulation); 18 U.S.C. § 371 (conspiracy to commit commodities fraud); 18 U.S.C. §§ 1343 and 1349 (wire fraud, securities fraud, and conspiracy to commit the same); 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957 (concealment money laundering, illegal money transferring, and conspiracy to commit the same), all in connection with a scheme to commit market manipulation on a platform called Mango Markets, then launder the proceeds (the "Subject Offenses"), including the following:

a. Records relating to the creation and users of the Subject Accounts and the Subject Servers;

b. Evidence of the creation and use of cryptocurrency wallets and accounts on cryptocurrency exchanges used in preparing for, perpetrating, or receiving funds from the Subject Offenses;

c. Evidence, including documents, images, and communications, reflecting any preparation for the Subject Offenses, including but not limited evidence reflecting research about manipulating cryptocurrency prices; research about potential targets for market manipulation; tests of purchasing and selling MNGO or MNGP Perpetuals; tests of transferring cryptocurrency to and from Mango Markets and other cryptocurrency exchanges used in the Subject Offenses; the planned steps in the Subject Offenses; the anticipated timing of the Subject Offenses; and planning for laundering funds from the Subject Offenses;

d. Evidence, including documents, images, and communications, reflecting acts in furtherance of the Subject Offenses and the transfer of funds obtained from the Subject Offenses;

e. Evidence, including documents, images, and communications, reflecting efforts to avoid to destroy or conceal information about the Subject Offenses, including but not limited to efforts to delete messages about the Subject Offenses and to prevent victims of the Subject Offenses from reporting information about the scheme to law enforcement;

f. Evidence, including documents, images, and communications, relating to AVRAHAM EISENBERG's relocation from the United States to Israel shortly after committing the Subject Offenses;

g. Evidence, including documents, images, and communications, reflecting AVRAHAM EISENBERG's knowledge of the laws prohibiting wire fraud, securities fraud,

commodities fraud, and market manipulations, including but not limited to evidence of EISENBERG's participation in lawsuits involving laws related to those subjects and EISENBERG's research or communication about lawsuits and criminal cases related to those subjects;

h. Evidence reflecting the identities of, and communications among, any co-conspirators in the Subject Offenses;

i. Evidence, including documents and communications, reflecting the state of mind of AVRAHAM EISENBERG and other participants in the Subject Offenses, including communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses;

j. Information that would assist in identifying and locating victims or witnesses;

k. Documents, spreadsheets, communications, and ledgers tracking cryptocurrency transfers and/or cryptocurrency payments;

l. Passwords or other information needed to access or identify computer or other online accounts, storage media, or other places where additional evidence, fruits, or instrumentalities of the Subject Offenses may be located;

m. Information pertaining to cryptocurrency digital wallets that may contain proceeds of the Subject Offenses;

n. Information relating to the ownership and disposition of criminal proceeds, including bank accounts, cryptocurrency wallets, accounts with centralized cryptocurrency exchanges, and other financial accounts;

o. Evidence relating to the use of financial accounts and transactions in furtherance of the Subject Offenses (including the means and methods used to obtain the accounts and funds therein, and how the transactions were undertaken);

p. Evidence concerning the technical expertise of AVRAHAM EISENBERG and any other participants in the Subject Offenses;

q. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place AVRAHAM EISENBERG and any co-conspirators and aiders and abettors in the Subject Offenses, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

r. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, payment for such online facilities or services, transfers of funds in furtherance of the Subject Offenses, and proceeds of the Subject Offenses; and

s. Evidence concerning any other online accounts, any computer devices or servers, or any other location where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with Multiple User
Accounts and a Server, Maintained at
Premises Controlled by Discord, Inc.,
USAO Reference No. 2022R00646

23 MAG 122**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Discord, Inc. (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent Brandon Racz of the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that the following Discord accounts (the “Subject Accounts”):

<u>User ID</u>	<u>Username(s)</u>
470697531823620116	AvrahamEisenberg#5451
281233046227779585	CrunchWrapSupreme#1469

And the following Discord server (the “Subject Server”):

<u>Server ID</u>	<u>Server Link</u>
782504674103656489	discord.gg/9RjPjCdGwK

All of which are maintained at premises controlled by Discord, Inc., headquartered at 444 De Haro Street, Suite 200, San Francisco, CA 94107, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to

provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, flight from prosecution, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of

this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

01/06/2023
Date Issued

5:10 p.m.
Time Issued


UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Email Search Attachment A

I. Subject Accounts, Subject Server, and Execution of Warrant

This warrant is directed to Discord, Inc. (the “Provider”), headquartered at 444 De Haro Street, Suite 200, San Francisco, CA 94107, and applies to all content and other information within the Provider’s possession, custody, or control associated with the following Discord accounts (collectively, the “Subject Accounts”):

<u>User ID</u>	<u>Username(s)</u>
470697531823620116	AvrahamEisenberg#5451
281233046227779585	CrunchWrapSupreme#1469

And the following server (the “Subject Server”):

<u>Server ID</u>	<u>Server Link</u>
782504674103656489	discord.gg/9RjPjCdGwK

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts and the Subject Server, for the period from **July 1, 2022 to the present**:

a. *Messaging content.* All public and private messages sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts and Subject Server, including all text,

attachments, and header information (specifically including the source and destination addresses associated with each communication, the date and time at which each communication was sent, and the size and length of each communication).

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts and Subject Servers.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts and Subject Servers, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts and Subject Servers, including any IP logs or other records of session times and durations.

e. *Deletion records.* All records reflecting deleted messages, including information about the account that deleted those messages and IP address from which the messages were deleted.

f. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts and Subject Servers, including complaints, inquiries, or other contacts with support services and records of actions taken.

g. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under Government control) are

authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1 (commodities fraud); 7 U.S.C. § 13(a)(2) (commodities and swap manipulation); 18 U.S.C. § 371 (conspiracy to commit commodities fraud); 18 U.S.C. §§ 1343 and 1349 (wire fraud, securities fraud, and conspiracy to commit the same); 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957 (concealment money laundering, illegal money transferring, and conspiracy to commit the same), all in connection with a scheme to commit market manipulation on a platform called Mango Markets, then launder the proceeds (the “Subject Offenses”), including the following:

- a. Records relating to the creation and users of the Subject Accounts and the Subject Servers;
- b. Evidence of the creation and use of cryptocurrency wallets and accounts on cryptocurrency exchanges used in preparing for, perpetrating, or receiving funds from the Subject Offenses;
- c. Evidence, including documents, images, and communications, reflecting any preparation for the Subject Offenses, including but not limited evidence reflecting research about manipulating cryptocurrency prices; research about potential targets for market manipulation; tests of purchasing and selling MNGO or MNGP Perpetuals; tests of transferring cryptocurrency to and from Mango Markets and other cryptocurrency exchanges used in the Subject Offenses; the planned steps in the Subject Offenses; the anticipated timing of the Subject Offenses; and planning for laundering funds from the Subject Offenses;
- d. Evidence, including documents, images, and communications, reflecting acts in furtherance of the Subject Offenses and the transfer of funds obtained from the Subject Offenses;

e. Evidence, including documents, images, and communications, reflecting efforts to avoid to destroy or conceal information about the Subject Offenses, including but not limited to efforts to delete messages about the Subject Offenses and to prevent victims of the Subject Offenses from reporting information about the scheme to law enforcement;

f. Evidence, including documents, images, and communications, relating to AVRAHAM EISENBERG's relocation from the United States to Israel shortly after committing the Subject Offenses;

g. Evidence, including documents, images, and communications, reflecting AVRAHAM EISENBERG's knowledge of the laws prohibiting wire fraud, securities fraud, commodities fraud, and market manipulations, including but not limited to evidence of EISENBERG's participation in lawsuits involving laws related to those subjects and EISENBERG's research or communication about lawsuits and criminal cases related to those subjects;

h. Evidence reflecting the identities of, and communications among, any co-conspirators in the Subject Offenses;

i. Evidence, including documents and communications, reflecting the state of mind of AVRAHAM EISENBERG and other participants in the Subject Offenses, including communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses;

j. Information that would assist in identifying and locating victims or witnesses;

k. Documents, spreadsheets, communications, and ledgers tracking cryptocurrency transfers and/or cryptocurrency payments;

l. Passwords or other information needed to access or identify computer or other online accounts, storage media, or other places where additional evidence, fruits, or instrumentalities of the Subject Offenses may be located;

m. Information pertaining to cryptocurrency digital wallets that may contain proceeds of the Subject Offenses;

n. Information relating to the ownership and disposition of criminal proceeds, including bank accounts, cryptocurrency wallets, accounts with centralized cryptocurrency exchanges, and other financial accounts;

o. Evidence relating to the use of financial accounts and transactions in furtherance of the Subject Offenses (including the means and methods used to obtain the accounts and funds therein, and how the transactions were undertaken);

p. Evidence concerning the technical expertise of AVRAHAM EISENBERG and any other participants in the Subject Offenses;

q. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place AVRAHAM EISENBERG and any co-conspirators and aiders and abettors in the Subject Offenses, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

r. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, payment for such online facilities or services, transfers of funds in furtherance of the Subject Offenses, and proceeds of the Subject Offenses; and

s. Evidence concerning any other online accounts, any computer devices or servers, or any other location where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with Three Google
Accounts, Maintained at Premises
Controlled by Google LLC, USAO
Reference No. 2022R00646

23 MAG 122

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google LLC (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

1. Warrant. Upon an affidavit of Special Agent Brandon Racz of the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that Google accounts associated with the following email addresses: (1) bochen.clean@gmail.com; (2) avi@thimessolutions.com; and (3) 613ike@gmail.com (collectively, the “Subject Accounts”), maintained and controlled by Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

01/06/2023

Date Issued

5:10 p.m.

Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Google Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Google LLC (the “Provider”), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Google accounts associated with the following email addresses: (1) bochen.clean@gmail.com; (2) avi@thimessolutions.com; and (3) 613ike@gmail.com (collectively, the “Subject Accounts”). A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account listed in Attachment A, for the period from **July 1, 2022 to the present**:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with, the Subject Accounts, including all message content (including all message content or attachments for emails sent in Google’s “confidential” mode), deleted content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of

each email, and the IP addresses of the sender and recipient of the email), as well as all forwarding and fetching accounts related to the Subject Account.

b. *Google Services Data.* The files and contents associated with the Subject Accounts related to the following Google Services: Gmail; Google Contacts; Google Messaging (including Google Hangouts); Google Drive; Google Docs; Google Reader; Google Voice; Google Photos; Google Chrome Sync; Google Calendar; Location History; Google Payments; and Google Maps.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, recovery and alternate email addresses, sign-in phone numbers, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Chrome Browser and web and search history records.* All records relating to Internet search and browsing history, and application usage history, including My Activity, Web & App Activity, device information history, and location history, including Chrome Browser records.

e. *Device Information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the Subject Account.

f. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.*

Any information identifying accounts that are associated with or connected to the Subject Account, including but not limited to specifically by cookies; recovery, secondary, forwarding, or alternate email address; Google ID; Android ID; IMEI; creation IP address; telephone number, including SMS recovery number or sign-in account number; or any other account or device identifier.

g. *Transactional records.* All transactional records associated with the Subject

Accounts, including any IP logs or other records of session times and durations, along with device information (including user agent strings) used to access the Subject Accounts.

h. *Customer correspondence.* All correspondence with the subscriber or others

associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

i. *Preserved or backup records.* Any preserved or backup copies of any of the

foregoing categories of records, whether created in response to a preservation request issued by the Government pursuant to 18 U.S.C. § 2703(f), or otherwise.

j. *Messages.* The contents of all instant messages associated with the Subject

Account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message.

k. *Files and Records.* The contents of all files and other records stored on the Subject

Accounts, including all device backups, all google and third-party app data, all files and other

records related to Google Mail, Google Photos, Chrome Tabs and Bookmarks, Google Drive, Google Voice, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under Government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of 7 U.S.C. §§ 9(1), 13(a)(5) and 17 C.F.R. § 180.1 (commodities fraud); 7 U.S.C. § 13(a)(2) (commodities and swap manipulation); 18 U.S.C. § 371 (conspiracy to commit commodities fraud); 18 U.S.C. §§ 1343 and 1349 (wire fraud, securities fraud, and conspiracy to commit the same); 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(h), and 1957 (concealment money laundering, illegal money transferring, and conspiracy to commit the same), all in connection with a scheme to commit market manipulation on a platform called Mango Markets, then launder the proceeds (the “Subject Offenses”), including the following:

- a. Records relating to the creation and users of the Subject Accounts and the Subject Servers;
- b. Evidence of the creation and use of cryptocurrency wallets and accounts on cryptocurrency exchanges used in preparing for, perpetrating, or receiving funds from the Subject Offenses;
- c. Evidence, including documents, images, and communications, reflecting any preparation for the Subject Offenses, including but not limited evidence reflecting research about manipulating cryptocurrency prices; research about potential targets for market manipulation; tests of purchasing and selling MNGO or MNGP Perpetuals; tests of transferring cryptocurrency to and

from Mango Markets and other cryptocurrency exchanges used in the Subject Offenses; the planned steps in the Subject Offenses; the anticipated timing of the Subject Offenses; and planning for laundering funds from the Subject Offenses;

d. Evidence, including documents, images, and communications, reflecting acts in furtherance of the Subject Offenses and the transfer of funds obtained from the Subject Offenses;

e. Evidence, including documents, images, and communications, reflecting efforts to avoid to destroy or conceal information about the Subject Offenses, including but not limited to efforts to delete messages about the Subject Offenses and to prevent victims of the Subject Offenses from reporting information about the scheme to law enforcement;

f. Evidence, including documents, images, and communications, relating to AVRAHAM EISENBERG's relocation from the United States to Israel shortly after committing the Subject Offenses;

g. Evidence, including documents, images, and communications, reflecting AVRAHAM EISENBERG's knowledge of the laws prohibiting wire fraud, securities fraud, commodities fraud, and market manipulations, including but not limited to evidence of EISENBERG's participation in lawsuits involving laws related to those subjects and EISENBERG's research or communication about lawsuits and criminal cases related to those subjects;

h. Evidence reflecting the identities of, and communications among, any co-conspirators in the Subject Offenses;

i. Evidence, including documents and communications, reflecting the state of mind of AVRAHAM EISENBERG and other participants in the Subject Offenses, including

communications reflecting false (purportedly exculpatory) explanations of any participant's involvement in the Subject Offenses;

j. Information that would assist in identifying and locating victims or witnesses;

k. Documents, spreadsheets, communications, and ledgers tracking cryptocurrency transfers and/or cryptocurrency payments;

l. Passwords or other information needed to access or identify computer or other online accounts, storage media, or other places where additional evidence, fruits, or instrumentalities of the Subject Offenses may be located;

m. Information pertaining to cryptocurrency digital wallets that may contain proceeds of the Subject Offenses;

n. Information relating to the ownership and disposition of criminal proceeds, including bank accounts, cryptocurrency wallets, accounts with centralized cryptocurrency exchanges, and other financial accounts;

o. Evidence relating to the use of financial accounts and transactions in furtherance of the Subject Offenses (including the means and methods used to obtain the accounts and funds therein, and how the transactions were undertaken);

p. Evidence concerning the technical expertise of AVRAHAM EISENBERG and any other participants in the Subject Offenses;

q. Location data, including but not limited to geolocation reporting and location history data and metadata associated with other files that would place AVRAHAM EISENBERG and any co-conspirators and aiders and abettors in the Subject Offenses, as well as the devices they used, in specific places at specific times, and would indicate the use of their devices during those times;

r. Information regarding the registration of other email accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, payment for such online facilities or services, transfers of funds in furtherance of the Subject Offenses, and proceeds of the Subject Offenses; and

s. Evidence concerning any other online accounts, any computer devices or servers, or any other location where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

EXHIBIT 1

Approved:

22 MAG 10337

THOMAS S. BURNETT/NOAH SOLOWIEJCZYK
Assistant United States Attorneys

Before: HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

- - - - -	X	
UNITED STATES OF AMERICA	:	<u>SEALED COMPLAINT</u>
- v. -	:	Violation of 7 U.S.C.
	:	§§ 9(1), 13(a)(2),
AVRAHAM EISENBERG,	:	13(a)(5); 17 C.F.R.
	:	\$ 180.1; 18 U.S.C. § 2
	:	
Defendant.	:	COUNTY OF OFFENSE:
	:	New York
- - - - -	X	

SOUTHERN DISTRICT OF NEW YORK, ss.:

BRANDON RACZ, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Commodities Fraud)

1. In or about October 2022, in the Southern District of New York and elsewhere, AVRAHAM EISENBERG, the defendant, willfully and knowingly, directly and indirectly, used and employed, and attempted to use and employ, in connection with a swap, a contract of sale of a commodity in interstate and foreign commerce, and for future delivery on and subject to the rules of a registered entity, a manipulative and deceptive device and contrivance, in contravention of Title 17, Code of Federal Regulations, Section 180.1, by: (1) using and employing, and attempting to use and employ, a manipulative device, scheme, and artifice to defraud; (2) making, and attempting to make, untrue and misleading statements of material fact and omitting to state material facts necessary in order to make the statements made not untrue or misleading; and (3) engaging, and attempting to engage in acts, practices, and courses of business which operated and

would operate as a fraud and deceit upon other persons, to wit, EISENBERG engaged in a scheme involving the intentional and artificial manipulation of the price of perpetual futures contracts on a cryptocurrency exchange called Mango Markets, and other manipulative and deceptive devices and contrivances.

(Title 7, United States Code, Sections 9(1) and 13(a)(5); Title 17, Code of Federal Regulations, Section 180.1; Title 18, United States Code, Section 2.)

COUNT TWO
(Commodities Manipulation)

2. In or about October 2022, in the Southern District of New York and elsewhere, AVRAHAM EISENBERG, the defendant, did knowingly and intentionally manipulate and attempt to manipulate the price of a commodity in interstate commerce, and for future delivery on and subject to the rules of a registered entity, and of a swap, to wit, EISENBERG engaged in a scheme involving the intentional and artificial manipulation of the price of perpetual futures contracts on a cryptocurrency exchange called Mango Markets.

(Title 7, United States Code, Section 13(a)(2); Title 18, United States Code, Section 2.)

The bases for my knowledge and for the foregoing charge are, in part, as follows:

3. I am a Special Agent with the FBI and I have been personally involved in the investigation of this matter. This affidavit is based upon my personal participation in the investigation, and my conversations with law enforcement officers, law enforcement employees, and witnesses, as well as a review of documents. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of this investigation. Where the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview of the Mango Markets Manipulation Scheme

4. As described in greater detail below, Mango Markets is a decentralized cryptocurrency exchange that has its own native crypto token, called MNGO. Investors can buy and sell MNGO and other cryptocurrencies on Mango Markets. Investors on Mango

Markets can also buy and sell perpetual futures ("Perpetuals") based on the relationship between the value of MNGO and the value of a crypto stablecoin called USD Coin ("USDC"), which is designed to be pegged to the dollar. Perpetuals are "swaps" under the Commodity Exchange Act. An investor who buys a Perpetual for MNGO stands to profit if the value of MNGO rises relative to the value of USDC, and an investor who sells a Perpetual for MNGO stands to profit if the value of MNGO falls relative to the value of USDC. Finally, Mango Markets allows investors to borrow cryptocurrency from the exchange, in amounts based on the value of the borrower's portfolio, and to withdraw that borrowed cryptocurrency.

5. As explained in greater detail below, in or about October 2022, AVRAHAM EISENBERG, the defendant, participated in a scheme to steal approximately \$110 million by artificially manipulating the price of MNGO Perpetuals on Mango Markets (the "Market Manipulation Scheme"). The scheme worked as follows: EISENBERG used an account that he controlled on Mango Markets to sell a large amount of Perpetuals for MNGO and used a separate account on Mango Markets to purchase those same Perpetuals. In other words, EISENBERG sold himself MNGO Perpetuals. EISENBERG then engaged in a series of large purchases of MNGO, with the objective of artificially increasing the price of MNGO relative to USDC, which had the effect of increasing the price of MNGO Perpetuals on Mango Markets. That purchasing achieved the desired effect, causing the price of MNGO Perpetuals on Mango Markets to increase precipitously over the course of approximately 20 minutes. Over that time span of approximately 20 minutes, the price of MNGO Perpetuals rose from approximately 0.0382 USDC/MNGO to approximately 0.54 USDC/MANGO, an increase of approximately 1300 percent.

6. As the price of MNGO Perpetuals on Mango Markets rose as a result of the Market Manipulation Scheme perpetrated by AVRAHAM EISENBERG, the defendant, the value of the MNGO Perpetuals that EISENBERG had purchased also rose. Because Mango Markets allows investors to borrow and withdraw cryptocurrency based on the value of their assets on the platform, the increase in the value of the MNGO Perpetuals EISENBERG had purchased allowed EISENBERG to borrow, then withdraw, approximately \$110 million worth of various cryptocurrencies from Mango Markets, which came from deposits of other investors in the Mango Markets exchange. When EISENBERG borrowed and withdrew that cryptocurrency, he had no intention to repay the borrowed funds. Accordingly, after EISENBERG borrowed and withdrew essentially all of the cryptocurrency deposits on the Mango Markets platform, EISENBERG ceased manipulating the price of MNGO Perpetuals, causing the price

of MNGO Perpetuals to fall significantly. Due to EISENBERG's withdrawals, other investors with deposits on Mango Markets lost much, or all, of those deposits.

Background on Mango Markets

7. Based on my training and experience, my participation in this investigation, my review of publicly available records (including the Mango Markets website), and my participation in discussions with individuals knowledgeable about Mango Markets, I have learned, in substance and in part, the following:

a. Mango Markets is a decentralized cryptocurrency exchange that allows investors to lend, borrow, swap, and leverage-trade cryptocurrency assets. Mango Markets is run by the Mango Decentralized Autonomous Organization (the "Mango DAO"). A decentralized autonomous organization, or "DAO," generally refers to an entity structure in which there is no central decision-making authority, and such authority is instead distributed across digital token holders, who cast votes to make decisions. In the context of the Mango DAO, for instance, holders of MNGO are allowed to vote on changes to Mango Markets and issues related to the governance of the Mango DAO, among other things.

b. To use Mango Markets, an investor must connect a cryptocurrency wallet to the exchange, create a Mango Markets account, and deposit cryptocurrency into that account. Once an investor has created and funded a Mango Markets account, the investor can trade different types of cryptocurrencies, including the MNGO token, on the Mango Markets exchange.

c. One type of trade investors can make is known as a "spot" trade. In a spot trade, an investor exchanges one cryptocurrency for another, at whatever the prevailing exchange rate between those two cryptocurrencies is at the time of the transaction. Investors can also make leveraged spot trades, in which the investor's deposits and other positions are used as collateral, allowing the investor to buy more of another cryptocurrency on margin than the investor could purchase through a one-for-one exchange.

d. Another type of trade available on Mango Markets is a perpetual futures contract, or "Perpetual" for short. When an investor buys or sells a Perpetual for a particular cryptocurrency, the investor is not buying or selling that cryptocurrency. Instead, the investor is buying or selling

exposure to future movements in the value of that cryptocurrency relative to another cryptocurrency. For example, if an investor buys a MNGO Perpetual at a price of 0.02 USDC/MNGO, the investor is "long" on MNGO, and the value of that perpetual will rise if the value of MNGO rise above 0.02 USDC/MNGO. Conversely, if an investor sells a MNGO Perpetual at a particular price, the investor is "short" on MNGO, and the value of that Perpetual will rise if the value of MNGO falls relative to USDC. Like with spot trading, investors on Mango Markets can also make leveraged Perpetuals trades, in which the investor's deposits and other positions act as collateral, thereby allowing the investor to buy a larger Perpetual position than the value of those deposits.

e. For the reasons given above, the price of a Perpetual at any particular time depends on, among other things, the relative value of two cryptocurrencies. To determine the relative value of cryptocurrency pairs for purpose of pricing Perpetuals, Mango Markets uses an "oracle," which is a computer program that calculates the relative value of cryptocurrency pairings by looking at the exchange rate of those cryptocurrencies on various cryptocurrency exchanges (the "Oracle"). When the Oracle price changes for a particular cryptocurrency pairing, the price of Perpetuals in that cryptocurrency pairing also changes on Mango Markets. Accordingly, changes in the relative price of cryptocurrency pairs on other exchanges impact the price of Perpetuals on the Mango Markets platform.

f. In addition to allowing investors to use deposits and other positions as collateral for leveraged trades, Mango Markets also allows investors to use those deposits and positions as collateral for borrowing and withdrawing cryptocurrency from the Mango Markets exchange. To borrow through Mango Markets, investors must access the Mango Markets website and click a button labeled "borrow" that allows the user to borrow cryptocurrency. The user can withdraw the cryptocurrency the user has borrowed by clicking another button labeled "withdraw." The cryptocurrency that investors borrow through Mango Markets comes from cryptocurrency that other investors have deposited in Mango Markets accounts.

g. The amount that an investor on Mango Markets can withdraw is determined by a formula that looks at, among other things, the value of the cryptocurrency deposited in the investor's account, the value of the investor's positions on Mango Markets, and the amount of cryptocurrency that the investor has already borrowed through Mango Markets. Mango Markets uses a formula to track the relationship between these assets and liabilities, which

Mango Markets labels the "health" of the account. If the "health" of a Mango Markets account falls below zero, the investor's positions on Mango Markets can be liquidated.

8. I understand that virtual currencies, such as USDC, are "commodities" under the Commodity Exchange Act ("CEA"). See, e.g., *C.F.T.C. v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018) ("A 'commodity' encompasses virtual currency both in economic function and in the language of the statute."); *United States v. Reed*, No. 20 Cr. 500 (JGK), 2022 WL 597180, at *3 (S.D.N.Y. Feb. 28, 2022) (finding "defendant had ample notice from the broad definition of commodities under the CEA that cryptocurrencies were within the definition of commodities"). Accordingly, Perpetuals based on the relative value of MNGO and USDC are "swaps" under the CEA. See 7 U.S.C. § 1(47) (A).

EISENBERG's Market Manipulation Scheme

9. Based on my review of records and data from a company called Circle, I have learned, in substance and in part, the following:

a. Circle provides a platform that allows individuals to create accounts, in which they can purchase, sell, store, and transfer the crypto stablecoin USDC.

b. In or about 2019, AVRAHAM EISENBERG, the defendant, opened an account at Circle ("Circle Account-1"). I know that EISENBERG is the user of Subject Account-1 because the account opener used the name "Avraham Eisenberg" and provided a photograph of EISENBERG's passport. I have reviewed that photograph and recognize the person pictured on the passport as EISENBERG.

10. Based on my review of publicly available trading data, data from a cryptocurrency exchange ("Exchange-1"), and data from Circle, I have learned that, on or about October 11, 2022, AVRAHAM EISENBERG, the defendant, created a large Perpetual position based on the relative value of MNGO and USDC by funding two Mango Markets accounts and selling a large amount of Perpetuals from one to the others. Specifically, I have learned, in substance and in part, the following:

a. On or about October 11, 2022, in the late morning and early afternoon,¹ Circle Account-1, which belongs to EISENBERG, sent approximately 14,179,322 USDC to a cryptocurrency wallet that then sent approximately 12,499,900 USDC to an account at Exchange-1 (the "Exchange-1 Account") which as explained below, is also controlled by EISENBERG.

b. Between approximately 3:36 p.m. and 3:50 p.m., Exchange-1 Account sent approximately 5,524,838 USDC to a cryptocurrency wallet ("Solana Wallet-1") on the blockchain known as Solana, which is the blockchain on which Mango Markets is built.

c. At approximately 3:47 p.m., the Exchange-1 Account sent approximately 4,999,999.95 USDC to another wallet on the Solana blockchain ("Solana Wallet-2").

d. Between approximately 6:08 p.m. and 6:18 p.m., the Exchange-1 Account sent approximately 5,000,100 USDC to a Mango Markets account ("Mango Account-1").

e. Between approximately 6:07 p.m. and 6:18 p.m., Solana Wallet-2 sent approximately 4,999,998.95 USDC to a different Mango Markets account ("Mango Account-2").

f. Between approximately 6:24 p.m. and 6:25 p.m., Mango Account-2 sold to Mango Account-1 Perpetuals based on the relative value of MNGO and USDC. The Perpetuals were based on a total of approximately 488,302,109 MNGO, at a price of 0.0382 USDC/MNGO. Accordingly, Mango Account-1 held a "long" position, the value of which would rise if the value of MNGO relative to USDC rose above 0.0382 USDC/MNGO (the "Long MNGO Perpetual Position"). Mango Account-2 held a "short" position, the value of which would rise if the value of MNGO relative to USDC fell below 0.0382 USDC/MNGO (the "Short MNGO Perpetual Position").

g. Because the USDC that funded both Mango Account-1 and Mango Account-2 originated with EISENBERG's account at Circle, it appears that EISENBERG controlled or at a minimum funded both Mango Account-1 and Mango Account-2. Accordingly, EISENBERG was on both sides of the MNGO Perpetual transaction described above.

¹ All times are in Eastern Time and, based on my review of travel records, I have learned that EISENBERG was in Puerto Rico at the time of the Market Manipulation Scheme.

11. As described in the following paragraphs, immediately after the creation of the Long and Short MNGO Perpetuals, AVRAHAM EISENBERG, the defendant, used USDC to purchase large amounts of MNGO on multiple cryptocurrency exchanges, which had the effect of artificially increasing the value of MNGO relative to USDC.

12. Based on my review of publicly available trading data on the Solana blockchain and my review of publicly available documents (including from Mango Markets), I have learned, in substance and in part, the following:

a. Aggregator-1 is a program that allows users to buy and sell cryptocurrency across a number of different cryptocurrency exchanges simultaneously. Aggregator-1 is available through the Mango Markets, as another way for Mango Markets investors to buy and sell cryptocurrency. One of the cryptocurrency exchanges through which Aggregator-1 transacts is one of the programs from which the Oracle gathered data for pricing Perpetuals.

b. As explained above, on or about October 11, 2022, Circle Account-1, which was the account belonging to AVRAHAM EISENBERG, the defendant, at Circle, sent USDC to the Exchange-1 Account, which then sent USDC to Solana Wallet-1.

c. Between approximately 6:26 p.m. and approximately 6:45 p.m., on or about October 11, 2022, the user of Solana Wallet-1 executed multiple transactions on Jupiter Aggregator, in which the user of Solana Wallet-1 sold USDC for a total of over 3.4 million MNGO.

d. At the same time as the user of Solana Wallet-1 was purchasing a large volume of MNGO through Aggregator-1, the value of MNGO relative to USDC rose from a low of approximately 0.0389 USDC/MNGO to a high of approximately 0.91 USDC/MNGO on the exchange utilized by the Oracle for pricing Perpetuals.

13. Based on my review of data and records from a cryptocurrency exchange that has offices in, among other locations, Manhattan, New York ("Exchange-2"), communications with representatives of Exchange-2, and publicly available documents (including from Mango Markets), I have learned, in substance and in part, the following:

a. Exchange-2 was one of the exchanges from which the Oracle gathered data for pricing Perpetuals.

b. On or about October 11, 2022, an individual opened and funded an anonymous account on Exchange-2 (the "Exchange-2 Account").

c. Between approximately 6:26 p.m. and approximately 6:45 p.m., the Exchange-2 Account sold USDT for over 1 million MNGO. During that period, the price of MNGO rose from a low of approximately 0.04 USDT/MNGO to a high of approximately 0.45 USDT/MNGO. Like USDC, USDT is a stablecoin designed to be pegged to the dollar.

d. I have learned that AVRAHAM EISENBERG, the defendant, controlled the Exchange-2 Account. Specifically, I have learned, in substance and in part, that following the Market Manipulation Scheme, Exchange-2 froze funds in the Exchange-2 Account, and EISENBERG initiated a legal action to try to retrieve the funds from the account, claiming to be the owner.

e. Opening, funding, and trading through Exchange Account-2 resulted in wires and data being transmitted to, among other locations, Exchange-2's office in Manhattan.

14. Based on my review of data and records from Exchange-1, records from Google, and publicly available documents (including from Mango Markets), I have learned, in substance and in part, the following:

a. Exchange-1 was one of the exchanges from which the Oracle gathered data for pricing Perpetuals.

b. As explained above, Circle Account-1, which belongs to AVRAHAM EISENBERG, the defendant, sent USDC to the Exchange-1 Account on or about October 11, 2022.

c. The Exchange-1 Account was opened on or about September 19, 2022, using a passport and personal identifying information that appears to belong to a Ukrainian woman, along with a particular Gmail address ("Gmail Address-1").

d. Nonetheless, it appears that the Exchange-1 Account is controlled by EISENBERG for the following reasons, among others:

i. As explained above, EISENBERG's Circle Account, Circle Account-1, sent over 12 million USDC to the Exchange-1 Account.

ii. Gmail Address-1, which was used to create the Exchange-1 Account, was created on or about September 1, 2022 – just a few weeks before the Exchange-1 Account was opened. The recovery email address for Gmail Address-1 is “avi@thimessolutions.com,” which is registered to EISENBERG. Similarly, the recovery phone number for Gmail Address-1 is the same phone number that EISENBERG listed as his contact phone number for Circle Account-1. Accordingly, it appears that EISENBERG actually controls Gmail Address-1, which was then used to create the Exchange-1 Account.

e. Between approximately 6:26 p.m. and 6:40 p.m., the Exchange-1 Account sold USDC for a total of over 16 million MNGO. During that period, the price of MNGO rose from a low of approximately 0.0388 USDC/MNGO to a high of approximately 0.1557 USDC/MNGO.

15. By artificially manipulating the value of MNGO relative to USDC, AVRAHAM EISENBERG, the defendant, also intended to and did increase the price of MNGO Perpetuals on Mango Markets, which significantly increased the value of the Long MNGO Perpetual Position that EISENBERG had purchased, thereby allowing EISENBERG to borrow and withdraw large amounts of cryptocurrency from Mango Markets. Specifically, based on my review of publicly available data from Mango Markets, I have learned, in substance and in part, the following:

a. As explained above, the price of Perpetuals on Mango Markets was set by the Oracle, which calculates the relative price of cryptocurrencies by looking at prices on other cryptocurrency exchanges.

b. During the trading described above, the price of Perpetuals based on the relative value of MNGO and USDC on Mango Markets rose significantly. Specifically, between approximately 6:26 p.m. and 6:45 p.m., on or about October 11, 2022, the price of MNGO Perpetuals on Mango Markets rose from approximately 0.0382 USDC/MNGO to a high of approximately 0.54 USDC/MNGO – an increase of over 1300 percent.

c. As the price of MNGO Perpetuals rose, the value of the Long MNGO Perpetual Position that Mango Account-1 had purchased rose, accordingly. Because of that increase in value, EISENBERG, who controlled Mango Account-1, was able to use the “borrow” and “withdraw” function on Mango Markets to borrow and

withdraw a large amount of cryptocurrency, without the "health" of Mango Account-1 dropping low enough to trigger liquidation.

d. Following that increase in borrowing power, EISENBERG borrowed and withdrew approximately \$110 million worth of different cryptocurrencies from Mango Markets. For example:

i. At approximately 6:29 p.m., Mango Account-1 borrowed and withdrew approximately 50,000,000 USDC from Mango Markets and sent those assets to Solana Wallet-1.

ii. At approximately 6:36 p.m., Mango Account-1 borrowed and withdrew approximately 400,000 SOL, which is the Solana cryptocurrency, from Mango Markets, and sent those assets to Solana Wallet-1.

iii. At approximately 6:37 p.m., Mango Account-1 borrowed and withdrew approximately 798,000 mSOL, which is a crypto token on the Solana blockchain, and approximately 282.12 wBTC, which is a cryptocurrency designed to track the value of Bitcoin, from Mango Markets.

iv. At approximately 6:41 p.m., Mango Account-1 borrowed and withdrew approximately 2,807,721 USDC and approximately 3,266,426 USDT, which is a cryptocurrency designed to track the value of the dollar, from Mango Markets, and sent those assets to Solana Wallet-1.

v. At approximately 6:45 p.m., Mango Account-1 borrowed and withdrew approximately 2,354,260 SRM, which is the native cryptocurrency for a platform called Serum, and approximately 32,409,565.06 MNGO, from Mango Markets, and sent those assets to Solana Wallet-1.

e. The cryptocurrency that EISENBERG borrowed and withdrew came from, among other places, the deposits and assets belonging to other Mango Markets investors. The user of Mango Account-1 withdrew effectively all available funds from Mango Markets.

f. While EISENBERG purported to be borrowing the cryptocurrency, he appeared to have no intention of actually repaying those loans. Following the withdrawals described above, Solana Wallet-1, the Exchange-1 Account, and the Exchange-2 Account ceased purchasing MNGO and began to sell MNGO for USDC. The price of MNGO tokens fell precipitously, causing the price of MNGO Perpetuals on Mango Markets to fall to approximately 0.02

USDC/MNGO. As a result, the Long MNGO Perpetual Position dropped to having a negative value and the "health" of Mango Account-1 fell below zero, making Mango Account-1 subject to liquidation. There was, however, nothing to liquidate because EISENBERG had already withdrawn the cryptocurrency.

EISENBERG Admits to the Market Manipulation Scheme

16. Based on my review of publicly available posts on a website where holders of MNGO can vote on Mango DAO proposals, as well as my communications with individuals who have knowledge of Mango DAO's operations, I have learned, in substance and in part, the following:

a. Between on or about October 11 and 13, 2022, representatives of Mango DAO engaged in negotiations with an individual purporting to be the perpetrator and others purporting to be in contact with the perpetrator. The negotiations focused on, among other things, the perpetrator returning some of the cryptocurrency from the attack.

b. Based on those negotiations, on or about October 13, 2022, members of the Mango DAO issued a written proposal on the Mango DAO message board and to the user of Solana Wallet-1. The proposal had, among other things, the following terms: (i) the Mango DAO would receive cryptocurrency worth approximately \$67 million from the user of Solana Wallet-1; (ii) the funds from the user of Solana Wallet-1 would, in combination with funds owned by the Mango DAO, be used to, among other things, repay Mango Market investors who had lost deposits; (iii) holders of MNGO would agree to waive certain civil claims and refrain from pursuing criminal investigations or attempting to freeze assets taken during the scheme. The proposal also called for the user of Solana Wallet-1 to make a 10,000,000 USDC payment to a wallet controlled by members of the Mango DAO, no later than 12 hours after the issuance of the proposal, and before a final vote.

c. On or about October 15, 2022, a cryptocurrency wallet on the Ethereum blockchain ("Ethereum Wallet-1") sent approximately 10 million USDC to a wallet controlled by members of the Mango DAO. Based on the proposal described above, it therefore appears that the user of Solana Wallet-1 also controls Ethereum Wallet-1.

d. After the transfer described, members of the Mango DAO voted to approve the October 13, 2022 proposal described

above. Following that approval, multiple cryptocurrency wallets sent the Mango DAO approximately \$57 million worth of cryptocurrency, in addition to the 10 million USDC that Mango DAO had already received.

e. Members of Mango DAO and Mango Markets did not receive the rest of the cryptocurrency that had been taken, which amounted to approximately \$40 million worth of different cryptocurrencies.

17. Shortly after the negotiations described above, AVRAHAM EISENBERG, the defendant, claimed responsibility for the Market Manipulation Scheme. Specifically, based on my review of publicly available information on Twitter, I have learned, in substance and in part, the following:

a. EISENBERG uses a particular Twitter account ("Twitter Account-1"). EISENBERG appears to be the user of Twitter Account-1 because the username of the account is "Avraham Eisenberg" and, in the past, Twitter Account-1 displayed a user photograph that I know was an image of EISENBERG based on my review of his passport photograph.

b. On or about October 15, 2022 – the same day as the repayment of some cryptocurrency as described above – Twitter Account-1 displayed a series of posts stating, in substance and in part, that the user of Twitter Account-1 had "operated a highly profitable trading strategy" that "took place on[] Mango Markets" and resulted in Mango Markets becoming "insolvent."²

c. Moreover, EISENBERG's posts on Twitter Account-1 show that he was aware of the laws prohibiting market manipulation. For example, on or about September 1, 2022, Twitter Account-1 posted a link to a press release from the United States Attorney's Office of the Southern District of New York, announcing charges, including under the CEA, in connection with a defendant artificially manipulating a foreign currency exchange rate in order to trigger a payment under an options contract.

18. Based on my review of travel records, I have learned that, on or about October 12, 2022 – the day after the Market Manipulation Scheme – AVRAHAM EISENBERG, the defendant, flew from

² The posts also stated, in substance and in part, that the user of Twitter Account-1 had helped negotiate an agreement to make users of Mango Markets whole and that the user of Twitter Account-1 believed all of his actions were legal.

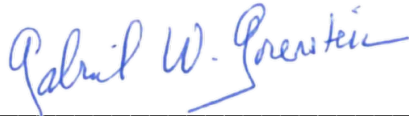
the United States to Israel. Based on the timing of the flight, the travel appears to have been an effort to avoid apprehension by law enforcement in the immediate aftermath of the Market Manipulation Scheme.

WHEREFORE, the deponent respectfully requests that a warrant be issued for the arrest of AVRAHAM EISENBERG, the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.

/s/ Brandon Racz (sworn telephonically)

BRANDON RACZ
Special Agent
FBI

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 4.1 and 41(d)(3), this
23rd th day of December, 2022



THE HONORABLE GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK